# Two non-orthogonal states can be cloned by a unitary-reduction process

Lu-Ming Duan* and Guang-Can Guo*
Department of Physics, University of Science
and Technology of China, Hefei, 230026, P.R.China

**Abstract**

We show that, there are physical means for cloning two non-orthogonal pure states which are secretly chosen from a certain set $\$ = \{|\Psi_0\rangle, |\Psi_1\rangle\}$. The states are cloned through a unitary evolution together with a measurement. The cloning efficiency can not attain 100%. With some negative measurement results, the cloning fails.

**PACS numbers:** 03.65.Bz, 89.70.+c, 02.50.-v

*E-mail: gcguo@sunlx06.nsc.ustc.edu.cn

The development of quantum information theory [1] draws attention to fundamental questions about what is physically possible and what is not. An example is the quantum no-cloning theorem [2], which asserts, unknown pure states can not be reproduced or copied by any physical means. Recently, there are growing interests in the no-cloning theorem. The original proof of this theorem [2] shows that the cloning machine violates the quantum superposition principle, which applies to a minimum total number of three states, and hence does not rule out the possibility of cloning two non-orthogonal states. Refs. [3] and [4] show that a violation of unitarity makes cloning two non-orthogonal states impossible. The result has also been extended to mixed states. That is the quantum no-broadcasting theorem [5], which states, two non-commuting mixed states can not be broadcast onto two separate quantum systems, even when the states need only be reproduced marginally. With the fact that quantum states can not be cloned ideally, recently, inaccurate copying of quantum states arouse great interests [6-9].

In this letter, we show that, however, there are physical means for cloning two non-orthogonal pure states. This does not contradict to the previous proofs of the no-cloning or no-broadcasting theorem. The proof in [2] applies to at least three states. Though the no-cloning theorem was extended to two states in [3] and [4], the proof only holds for the unitary evolution, not for any physical means. In particular, measurements are not considered. Similarly, the no-broadcasting theorem proven in [5] is also limited to the unitary evolution. ( This time it is a generalized unitary evolution by introducing an ancillary system. ) To show this, we note in the proof the inequality

$$F\left(\rho_0,\rho_1\right)\leq F\left(\widetilde{\rho}_0,\widetilde{\rho}_1\right) \tag{1}$$

plays an essential role, ( Eq. (17) in Ref. [5] ), where $\rho_s$ and $\widetilde{\rho}_s$ $(s=0,1)$ are the density operators before and after the evolution, respectively. $F$ indicates the fidelity, which is defined by

$$F\left(\rho_0,\rho_1\right)=tr\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}. \tag{2}$$

In Ref. [5], the inequality (1) was proven for the general unitary evolution. Though there is a theorem in [10], which states, the fidelity (2) does not decrease through measurements, the proof exclude the "read-out" (or the projection) step.

So the evolution there is still a general unitary evolution, not a real measurement. In fact, the inequality (1) is not true for the measurement process. We show it by the following example.

Consider two pure states $|\Psi_0\rangle$ and $|\Psi_1\rangle$, which are defined by

$$\begin{aligned} |\Psi_0\rangle &= \tfrac{1}{\sqrt{2}}\left(|s_1\rangle + |s_3\rangle\right), \\ |\Psi_1\rangle &= \tfrac{1}{\sqrt{2}}\left(|s_2\rangle + |s_3\rangle\right), \end{aligned} \tag{3}$$

where $|s_1\rangle$, $|s_2\rangle$, and $|s_3\rangle$ are three eigenstates of an observable $S$ with the eigenvalues $s_1$, $s_2$, and $s_3$, respectively. We measure the observable $S$. If the measurement result is $s_3$, the output state is discarded. With the input states $|\Psi_0\rangle$ and $|\Psi_1\rangle$, the output states are respectively

$$\begin{aligned} \left|\widetilde{\Psi}_0\right\rangle &= |s_1\rangle, \\ \left|\widetilde{\Psi}_1\right\rangle &= |s_2\rangle. \end{aligned} \tag{4}$$

It is obvious that

$$F\left(\rho_0, \rho_1\right) = |\langle\Psi_0|\Psi_1\rangle| = \frac{1}{2} > 0 = F\left(\widetilde{\rho}_0, \widetilde{\rho}_1\right). \tag{5}$$

So the inequality (1) does not hold for the measurement process.

Now we prove that two non-orthogonal state can be cloned by a unitary evolution together with a measurement. The result, posed formally, is the following theorem

*Theorem.* If $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are two non-orthogonal states of a quantum system A ,there exist a unitary evolution $U$ and a measurement $M$, which together yield the following evolution

$$\begin{aligned} |\Psi_0\rangle|\Sigma\rangle &\xrightarrow{U+M} |\Psi_0\rangle|\Psi_0\rangle, \\ |\Psi_1\rangle|\Sigma\rangle &\xrightarrow{U+M} |\Psi_1\rangle|\Psi_1\rangle, \end{aligned} \tag{6}$$

where $|\Sigma\rangle$ is the input state of a system B. Systems A and B each have an $n$-dimensional Hilbert space.

*Proof.* First we consider the measurement. If there exists a unitary operator $U$ to make

$$\begin{aligned} U\left(|\Psi_0\rangle|\Sigma\rangle|m_0\rangle\right) &= a_{00}|\Psi_0\rangle|\Psi_0\rangle|m_0\rangle + a_{01}|\Phi_{AB}\rangle|m_1\rangle, \\ U\left(|\Psi_1\rangle|\Sigma\rangle|m_0\rangle\right) &= a_{10}|\Psi_1\rangle|\Psi_1\rangle|m_0\rangle + a_{11}|\Phi_{AB}\rangle|m_1\rangle, \end{aligned} \tag{7}$$

where $|m_0\rangle$ and $|m_1\rangle$ are two orthogonal states of a probe P, in succession we measure the probe P, and the states are preserved if the measurement result is $m_0$. This measurement projects the composite system AB into the state $|\Psi_s\rangle\,|\Psi_s\rangle$, where $s=0$ or 1. So the evolution (6) exists if Eq. (7) holds. To prove existence of the unitary operator $U$ described by Eq. (7), we first introduce two lemmas.

*Lemma 1.* If the normalized states $|\phi_0\rangle$, $|\phi_1\rangle$, $\left|\widetilde{\phi}_0\right\rangle$, and $\left|\widetilde{\phi}_1\right\rangle$ satisfy $\langle\phi_0|\phi_1\rangle = \left\langle\widetilde{\phi}_0|\widetilde{\phi}_1\right\rangle = 0$, there exists a unitary operator $U$ to make

$$\begin{aligned} U\,|\phi_0\rangle &= \left|\widetilde{\phi}_0\right\rangle, \\ U\,|\phi_1\rangle &= \left|\widetilde{\phi}_1\right\rangle. \end{aligned} \tag{8}$$

*Proof:* Suppose the considered system has an $n$-dimensional Hilbert space $H$. There exist $n-2$ orthogonal states $|\phi_2\rangle$, $|\phi_3\rangle$, $\cdots$, $|\phi_{n-1}\rangle$ , which together with $|\phi_0\rangle$ and $|\phi_1\rangle$ make an orthonormal basis for the space $H$. Similarly, the states $\left|\widetilde{\phi}_0\right\rangle$, $\left|\widetilde{\phi}_1\right\rangle$, $\cdots$, and $\left|\widetilde{\phi}_{n-1}\right\rangle$ make another orthonormal basis. The following operator

$$U = \left|\widetilde{\phi}_0\right\rangle\langle\phi_0| + \left|\widetilde{\phi}_1\right\rangle\langle\phi_1| + \cdots + \left|\widetilde{\phi}_{n-1}\right\rangle\langle\phi_{n-1}| \tag{9}$$

is unitary, which can be easily checked by verifying the identity

$$UU^{+} = U^{+}U = I. \tag{10}$$

The operator $U$ defined by Eq. (9) evolves the states $|\phi_0\rangle$ and $|\phi_1\rangle$ into $\left|\widetilde{\phi}_0\right\rangle$ and $\left|\widetilde{\phi}_1\right\rangle$, respectively. Lemma 1 is thus proved.

*Lemma 2.* If the states $|\phi_0\rangle$, $|\phi_1\rangle$, $\left|\widetilde{\phi}_0\right\rangle$, and $\left|\widetilde{\phi}_1\right\rangle$ satisfy

$$\begin{aligned} \langle\phi_0|\phi_0\rangle &= \left\langle\widetilde{\phi}_0|\widetilde{\phi}_0\right\rangle, \\ \langle\phi_1|\phi_1\rangle &= \left\langle\widetilde{\phi}_1|\widetilde{\phi}_1\right\rangle, \\ \langle\phi_0|\phi_1\rangle &= \left\langle\widetilde{\phi}_0|\widetilde{\phi}_1\right\rangle, \end{aligned} \tag{11}$$

there exists a unitary operator $U$ to make $U\,|\phi_0\rangle = \left|\widetilde{\phi}_0\right\rangle$, and $U\,|\phi_1\rangle = \left|\widetilde{\phi}_1\right\rangle$.

*Proof:* Suppose $\gamma_0 = \||\phi_0\rangle\|$, and $\gamma_1 = \left\||\phi_1\rangle - \frac{\langle\phi_0|\phi_1\rangle}{\gamma_0^2}|\phi_0\rangle\right\|$, where the norm $\||\phi\rangle\|$ is defined by $\||\phi\rangle\| = \sqrt{\langle\phi|\phi\rangle}$. The normalized states $\frac{1}{\gamma_0}|\phi_0\rangle$ and $\frac{1}{\gamma_1}\left(|\phi_1\rangle - \frac{\langle\phi_0|\phi_1\rangle}{\gamma_0^2}|\phi_0\rangle\right)$ are obviously orthogonal. On the other hand, following Eq. (11), the two states $\frac{1}{\gamma_0}\left|\widetilde{\phi}_0\right\rangle$ and $\frac{1}{\gamma_1}\left(\left|\widetilde{\phi}_1\right\rangle - \frac{\langle\phi_0|\phi_1\rangle}{\gamma_0^2}\left|\widetilde{\phi}_0\right\rangle\right)$ are also normalized

and orthogonal. Hence, from Lemma 1 , there exists a unitary operator $U$ to make

$$\begin{aligned} U\left(\frac{1}{\gamma_0}\left|\phi_0\right\rangle\right) &= \frac{1}{\gamma_0}\left|\widetilde{\phi}_0\right\rangle, \\ U\left(\frac{1}{\gamma_1}\left(\left|\phi_1\right\rangle - \frac{\langle\phi_0|\phi_1\rangle}{\gamma_0^2}\left|\phi_0\right\rangle\right)\right) &= \frac{1}{\gamma_1}\left(\left|\widetilde{\phi}_1\right\rangle - \frac{\langle\phi_0|\phi_1\rangle}{\gamma_0^2}\left|\widetilde{\phi}_0\right\rangle\right). \end{aligned} \tag{12}$$

Eq. (12) is just another expression of the evolution $U\left|\phi_0\right\rangle = \left|\widetilde{\phi}_0\right\rangle$ and $U\left|\phi_1\right\rangle = \left|\widetilde{\phi}_1\right\rangle$. Lemma 2 is therefore proved.

Now we return to the proof of the main theorem. Let

$$\begin{aligned} \left|\phi_s\right\rangle &= \left|\Psi_s\right\rangle\left|\Sigma\right\rangle\left|m_0\right\rangle, \\ \left|\widetilde{\phi}_s\right\rangle &= a_{s0}\left|\Psi_s\right\rangle\left|\Psi_s\right\rangle\left|m_0\right\rangle + a_{s1}\left|\Phi_{AB}\right\rangle\left|m_1\right\rangle, \end{aligned} \tag{13}$$

where $s = 0$ or 1. Without loss of generality, here and in the following we suppose $\langle\Psi_0|\Psi_1\rangle$ is a positive real number. It can be easily checked that, if the constants $a_{00}$, $a_{01}$, $a_{10}$, and $a_{11}$ in Eq. (7) have the following values

$$\begin{aligned} a_{00} = a_{10} &= \frac{1}{\sqrt{1+\langle\Psi_0|\Psi_1\rangle}}, \\ a_{01} = a_{11} &= \frac{\sqrt{\langle\Psi_0|\Psi_1\rangle}}{\sqrt{1+\langle\Psi_0|\Psi_1\rangle}}, \end{aligned} \tag{14}$$

the states $\left|\phi_0\right\rangle$, $\left|\phi_1\right\rangle$, $\left|\widetilde{\phi}_0\right\rangle$, and $\left|\widetilde{\phi}_1\right\rangle$ defined by Eq. (13) satisfy the condition (11). So there exists a unitary operator $U$ to realize the evolution (7). This completes the proof of the main theorem.

The above proof of the theorem is constructive, i.e., it gives a method for constructing the desired unitary operator $U$ and the measurement $M$. We illustrate the construction by the following example.

*Example.* We consider the simplest system which consists of three parts, A and B and a probe P, each being a qubit ( a two-state quantum system ). We want to clone two non-orthogonal states $\left|\Psi_0\right\rangle$ and $\left|\Psi_1\right\rangle$ of the qubit A with $\langle\Psi_0|\Psi_1\rangle = \cos(\theta) = \tan^2\alpha$, where $0 \le \alpha < \frac{\pi}{4}$. For this system, the states in Eq. (7) can be chosen as $\left|\Psi_0\right\rangle = \left|0\right\rangle$, $\left|\Psi_1\right\rangle = \cos(\theta)\left|0\right\rangle + \sin(\theta)\left|1\right\rangle$, $\left|\Sigma\right\rangle = \left|0\right\rangle$, $\left|m_0\right\rangle = \left|0\right\rangle$, $\left|m_1\right\rangle = \left|1\right\rangle$, $\left|\Phi_{AB}\right\rangle = \left|00\right\rangle$ . We measure the qubit P. With the measurement result 0, the states of the qubit A are successfully cloned. According to Eq. (9), the unitary operator $U$ has the form $U = \sum_{i=0}^{7}\left|\widetilde{\phi}_i\right\rangle\left\langle\phi_i\right|$. A natural choice of the states $\left|\phi_i\right\rangle$ is the computational basis $\left|000\right\rangle$, $\left|100\right\rangle$, $\cdots$, $\left|111\right\rangle$. From Eq. (14) and the

proof of Lemma 2, the states $\left|\widetilde{\phi}_0\right\rangle$ and $\left|\widetilde{\phi}_1\right\rangle$ are respectively

$$\left|\widetilde{\phi}_0\right\rangle = \cos\alpha\left|000\right\rangle + \sin\alpha\left|001\right\rangle,$$

$$\left|\widetilde{\phi}_1\right\rangle = -\sqrt{\cos(2\alpha)}\sin\alpha\tan\alpha\left|000\right\rangle + \sin\alpha\tan\alpha\left(\left|100\right\rangle + \left|010\right\rangle\right) \tag{15}$$

$$+\sqrt{1-\tan^2\alpha}\left|110\right\rangle + \sqrt{\cos(2\alpha)}\sin\alpha\left|001\right\rangle.$$

$\left|\widetilde{\phi}_0\right\rangle$ and $\left|\widetilde{\phi}_1\right\rangle$ are superpositions of the states $\left|\phi_0\right\rangle$, $\left|\phi_1\right\rangle$, $\cdots$, and $\left|\phi_4\right\rangle$, so the three states $\left|\widetilde{\phi}_5\right\rangle$, $\left|\widetilde{\phi}_6\right\rangle$, and $\left|\widetilde{\phi}_7\right\rangle$ can be chosen as $\left|\phi_5\right\rangle$, $\left|\phi_6\right\rangle$, $\left|\phi_7\right\rangle$, respectively. The states $\left|\widetilde{\phi}_2\right\rangle$, $\left|\widetilde{\phi}_3\right\rangle$, and $\left|\widetilde{\phi}_4\right\rangle$ are also superpositions of the states $\left|\phi_0\right\rangle$, $\left|\phi_1\right\rangle$, $\cdots$, $\left|\phi_4\right\rangle$. The superposition constants are determined by the orthonormal conditions. This evolution leaves the subspace spanned by $\left|\phi_5\right\rangle$, $\left|\phi_6\right\rangle$, and $\left|\phi_7\right\rangle$ unchanged, and makes a rotation in the subspace spanned by $\left|\phi_0\right\rangle$, $\left|\phi_1\right\rangle$, $\cdots$, $\left|\phi_4\right\rangle$. The evolution $U$ can be fulfilled by the quantum controlled-NOT gates together with some single-qubit rotation gates [11,12]. From this example, we see, even for the simplest system, the evolution yielding the cloning is rather complicated.

At the first glance, that two non-orthogonal states can be cloned seemingly threatens the security of the quantum cryptography schemes based on non-orthogonal states [13-15]. But this is not the case. The key reason is that, though two non-orthogonal states can be cloned, they can not be cloned always successfully. If the measurement of the probe does not yield the desired result $m_0$, the cloning fails. Through these failures, Alice (the sender) and Bob ( the receiver) can find the intervention of Eve (the eavesdropper).

In Eq. (7), with probability $\eta_0 = a_{00}^2$ and $\eta_1 = a_{10}^2$, the measurement of the probe yields the desired cloned states for the composite system AB. So $\eta_0$ and $\eta_1$ define the cloning efficiencies. Now we prove that, for any cloning machines, the cloning efficiencies can not attain 100% at the same time. They must satisfy some basic inequalities.

A general unitary transformation of pure states can be decomposed as

$$\begin{aligned} U\left(\left|\Psi_0\right\rangle\left|\Sigma\right\rangle\left|m_p\right\rangle\right) &= \sqrt{\eta_0}\left|\Psi_0\right\rangle\left|\Psi_0\right\rangle\left|m_0\right\rangle + \sqrt{1-\eta_0}\left|\Phi_{ABP}^0\right\rangle, \\ U\left(\left|\Psi_1\right\rangle\left|\Sigma\right\rangle\left|m_p\right\rangle\right) &= \sqrt{\eta_1}\left|\Psi_1\right\rangle\left|\Psi_1\right\rangle\left|m_1\right\rangle + \sqrt{1-\eta_1}\left|\Phi_{ABP}^1\right\rangle, \end{aligned} \tag{16}$$

where $\left|m_p\right\rangle$, $\left|m_0\right\rangle$, and $\left|m_1\right\rangle$ are states of the probe, and $\left|\Phi_{ABP}^0\right\rangle$ and $\left|\Phi_{ABP}^1\right\rangle$ are two states of the composite system ABP. In general, they are not necessarily

orthogonal to each other. In the cloning, a measurement projects the states of the probe into the subspace spanned by $|m_0\rangle$ and $|m_1\rangle$. After projection, the state of the system AB should be $|\Psi_s\rangle\,|\Psi_s\rangle$, where $s = 0$ or 1. This requires

$$\left\langle m_0|\Phi^0_{ABP}\right\rangle = \left\langle m_1|\Phi^0_{ABP}\right\rangle = \left\langle m_0|\Phi^1_{ABP}\right\rangle = \left\langle m_1|\Phi^1_{ABP}\right\rangle = 0. \tag{17}$$

The above condition suggests that the cloning here is different from the inaccurate quantum copying in Ref. [7], where one does not need to require $\langle m_1|\Phi^0_{ABP}\rangle = \langle m_0|\Phi^1_{ABP}\rangle = 0$. With the condition (17), inner product of the two parts of Eq. (16) gives

$$\begin{aligned} &\langle\Psi_0|\Psi_1\rangle - \sqrt{\eta_0\eta_1}\,\langle\Psi_0|\Psi_1\rangle^2\,\langle m_0|m_1\rangle \\ &= \sqrt{(1-\eta_0)(1-\eta_1)}\,\langle\Phi^0_{ABP}|\Phi^1_{ABP}\rangle \\ &\leq \sqrt{(1-\eta_0)(1-\eta_1)}. \end{aligned} \tag{18}$$

In Eq. (18), we use the inequality $|\langle\Phi^0_{ABP}|\Phi^1_{ABP}\rangle| \leq \||\Phi^0_{ABP}\rangle\|\,\||\Phi^1_{ABP}\rangle\|$. From Eq. (18) , it is not difficult to obtain that

$$\frac{\eta_0+\eta_1}{2} \leq \frac{1-\langle\Psi_0|\Psi_1\rangle}{1-\langle\Psi_0|\Psi_1\rangle^2\langle m_0|m_1\rangle} \leq \frac{1}{1+\langle\Psi_0|\Psi_1\rangle}. \tag{19}$$

We have supposed $\langle\Psi_0|\Psi_1\rangle \neq 1$. This inequality suggests that the efficiencies $\eta_0$ and $\eta_1$ can not attain 100% at the same time for two non-orthogonal states. The equality in Eq. (19) holds if and only if $\eta_0 = \eta_1$ and $|m_0\rangle = |m_1\rangle$. The case $\eta_0 = \eta_1$ is of special interest. In this case, the cloning efficiency is independent of the input states. Such a cloning machine is called the universal quantum cloning machine. With $\eta_0 = \eta_1 = \eta$, Eq. (19) reduces to

$$\eta \leq \frac{1}{1+\langle\Psi_0|\Psi_1\rangle}. \tag{20}$$

Hence the efficiency given by Eq. (14) is in fact the maximum efficiency able to be obtained by a cloning machine. Also, for the universal cloning machine, the cloning efficiency is always less than 100%. This explains the security of the quantum cryptography schemes based on two non-orthogonal states [13-15]. The reason is not that non-orthogonal states can not be cloned, but that the cloning efficiency can not attain 100%.

**Acknoledgment**

This project was supported by the National Natural Science Foundation of China.

## References


[1] C.H.Bennett, Phys. Today 48, No. 10, 24 (1995).

[2] W.K. Wootters and W.H. Zurek, Nature (London) 299, 802 (1982).

[3] H.P. Yuen, Phys. Lett. A 113, 405 (1986).

[4] G.M. D'Ariano and H.P. Yuen, Phys. Rev. Lett. 76, 2832 (1996).

[5] H. Barnum, G.M. Caves, C.A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. 76, 2818 (1996).

[6] V. Buzek and M. Hillery, Phys. Rev. A 54, 1844 (1996).

[7] M. Hillery and V. Buzek, Los Alamos eprint archives quant-ph/9701034.

[8] V. Buzek, V.Vedral, M. Plenio, P.L. Knight, and M. Hillery, Los Alamos eprint archives quant-ph/9701028.

[9] V. Buzek, S.L. Braunstein, M. Hillery, and D. Bruss, Los Alamos eprint archives quant-ph/9703046.

[10] R. Jozsa, J. Mod. Opt. 41, 2315 (1994).

[11] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A 52, 3457 (1995).

[12] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. 74, 4083 (1995).

[13] C. H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. 68, 557 (1992).

[14] C.H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).

[15] M. Koashi and N. Imoto, Phys. Rev. Lett. 77, 2137 (1996).